What is claimed is:

1. A method for encrypting an input data string comprising a plurality of bits of binary data, the method comprising:

(a) generating a control code in response to the input data string;

(b) generating a position code in response to the control code; and

(c) combining the control code and the position code to form an encrypted data string;

wherein the control code indicates the order in which 2^n different configurations of n bits are identified in the position code and the position code indicates the position of the 2^n different configurations of n bits with respect to the input data string.

2. The method of claim 1, wherein step (a) comprises generating a control code in response to a control code index.

3. The method of claim 1, wherein step (a) comprises generating a control code in response to a predetermined default control code.

4. The method of claim 1, wherein step (b) comprises:

identifying and recording the position of the 2^n different configurations of n bits in an order determined in response to the control code.

5. The method of claim 1, further comprising dividing the input data string into a plurality of blocks of data comprising a number of bits of data prior to step (a).

6. The method of claim 5, wherein the number of bits within the plurality of blocks of data is determined in response to a random number generator.

7. The method of claim 5, wherein the number of bits within the plurality of blocks of data is determined in response to a mathematical formula.

8. The method of claim 5, further comprising generating a plurality of block codes indicating the number of bits within each block of data.

9. The method of claim 5, further comprising combining the plurality of block codes with the control code and the position code.

10. The method of claim 5, further comprising the step of:

analyzing one of said plurality of blocks of data by determining the relative frequencies of combinations of said bits of data to generate said control code,

analyzing said one of said plurality of blocks by determining whether a specific relationship exists between the combinations of said bits of data to predict whether said input data string can be compressed simultaneously as it is encrypted, and

identifying the position of the combinations of said bits of data by determining whether each of the combinations of said bits of data matches successive groups of said bits of data.

11. A method for encrypting an input data string comprising a plurality of bits of binary data, the method comprising:

(a) analyzing the input data string;

(b) generating a control code in response to the analysis of step (a) and in response to a control code index;

(c) generating a position code in response to the control code; and

(d) combining the control code and the position code to form an encrypted data string;

wherein the control code indicates the order in which 2^n different configurations of n bits are identified in the position code and the position code indicates the position of the 2^n different configurations of n bits with respect to the input data string.

12. The method of claim 11, wherein step (a) comprises dividing the input data string into a plurality of blocks of data comprising a number of bits of data.

13. The method of claim 12, further comprising generating a plurality of block codes indicating the number of bits of data within each block of data.

14. The method of claim 12, wherein the number of bits of data within the plurality of blocks of data is determined in response to a random number generator.

15. The method of claim 12, wherein the number of bits of data within the plurality of blocks of data is determined in response to a mathematical formula.

16. The method of claim 11 wherein step (a) comprises determining the relative frequencies

of the 2^n different configurations of n bits.

17. The method of claim 11, wherein step (a) comprises determining whether or not a predetermined relationship exists between the 2^n different combinations of n bits.

18. The method of claim 11, wherein step (a) comprises generating a control code in response to a control code index.

19. The method of claim 11, wherein step (a) comprises generating a control code in response to a predetermined default control code.

20. The method of claim 11, wherein step (b) comprises:

identifying and recording the position of the 2^n different configurations of n bits in an order determined in response to the control code.

21. A method for encrypting an input data string comprising a plurality of bits of binary data, the method comprising:

(a) using a software program code means embodied on a computer readable medium, analyzing the input data string;

(b) using a software program code means embodied on a computer readable medium, generating a configuration control code in response to the analysis of step (a) and in response to a control code index;

(c) using a software program code means embodied on a computer readable medium,

generating a position code in response to the control code; identifying the position of each n bit configuration in the data string;

wherein the control code indicates the order in which 2^n different configurations of n bits are identified in the position code and the position code indicates the position of the 2^n different configurations of n bits with respect to the input data string.

22. The method of claim 21, further comprising using a software program code means embodied on a computer readable medium, arranging the input data string into a plurality of data blocks prior to step (a).

23. A computer usable medium for encrypting an input data string comprising a plurality of bits of binary data, the medium comprising:

computer readable program code for analyzing the input data string;

computer readable program code for generating a control code in response to the analysis of step (a) and in response to a control code index;

computer readable program code for generating a position code in response to the control code; and

computer readable program code for combining the control code and the position code to form an encrypted data string;

wherein the control code indicates the order in which 2^n different configurations of n bits are identified in the position code and the position code indicates the position of the 2^n different configurations of n bits with respect to the input data string.